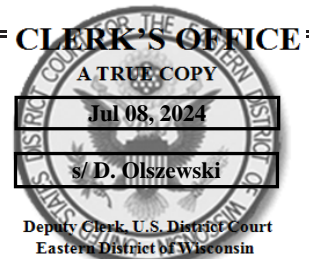


## UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

## In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

the person of Marcus M. FRANKLIN (DOB XX/XX/2005); a 2020  
Nissan Sentra four door sedan (VIN JN1AB8DV1LY205634, bearing  
Wisconsin license plate no. ATJ7945); and the premises located at 630  
N. Vel R. Phillips, Unit 812, Milwaukee, Wisconsin, ("PREMISES") as  
further described in Attachment A

Case No. 24 MJ 141

**APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Please see Attachment A.

located in the \_\_\_\_\_ Eastern \_\_\_\_\_ District of \_\_\_\_\_ Wisconsin \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 922(a)(1)(A);	engaging in the business of dealing and manufacturing of firearms without a
18 U.S.C. § 922(a)(5);	license; unlawful interstate transfer of a firearm; conspiracy
18 U.S.C. § 371	

The application is based on these facts:

Please see Affidavit.

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


  
 Applicant's signature

Sean Carlson, Special Agent - ATF

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
 \_\_\_\_\_ telephone \_\_\_\_\_ (specify reliable electronic means).

Date: 07/08/2024

  
 Judge's signature

City and state: Milwaukee, WI

Honorable William E. Duffin, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF  
APPLICATION FOR A SEARCH WARRANT**

I, Sean Carlson, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the following: the person of Marcus M. FRANKLIN (DOB XX/XX/2005); a 2020 Nissan Sentra four door sedan (VIN JN1AB8DV1LY205634, bearing Wisconsin license plate no. ATJ7945); and the premises located at 630 N. Vel R. Phillips, Unit 812, Milwaukee, Wisconsin, (“**PREMISES**”) as further described in Attachment A, for the items described in Attachment B.

2. I am employed as a Special Agent with the United States Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives (“ATF”) assigned to the Milwaukee Field Office since November 2015. I have been employed as a full-time law enforcement officer for approximately fifteen years. Prior to my employment at ATF, I was a Patrol Officer at the Hammond Police Department in Hammond, Indiana, for over four (4) years, and then I served approximately five (5) years as a Federal Air Marshal with the U.S. Department of Homeland Security.

3. As a Special Agent, I have participated in the investigation of firearms and narcotics-related offenses, resulting in the prosecution and conviction of numerous individuals and the seizure of illegal drugs, and weapons. As a firearms investigator, I have interviewed many individuals involved in firearm and drug trafficking and have obtained information from them regarding acquisition, sale, importation, manufacture, and distribution of firearms and controlled substances. Through my training and experience, I am familiar with the actions, habits, traits,

methods, and terminology utilized by the traffickers and abusers of controlled substances.

4. Based on my training, experience and participation in drug trafficking and firearms trafficking investigations, I know and have observed the following:

- i. I have relied on informants to investigate firearms trafficking and drug trafficking. Through informant interviews and debriefings of individuals involved in those offenses, I have learned about the manner in which individuals and organizations finance, purchase, transport, and distribute firearms and narcotics both within and outside of Wisconsin. I have utilized informants to conduct “controlled purchases” of firearms and controlled substances from individuals, as opposed to licensed gun dealers. I have also conducted surveillance of individuals engaged in firearms and drug trafficking and participated in the execution of numerous search warrants resulting in the seizure of drugs, firearms, ammunition, and magazines.
- ii. Based on my training and experience, I have become familiar with the language utilized over the telephone to discuss firearms and drug trafficking and know that the language is often limited, guarded, and coded. I also know that firearms and drug traffickers often use electronic devices (such as computers and cellular phones) and social media to facilitate these crimes. Based on my experience, I know that firearms traffickers may keep photographs of these items on electronic devices.
- iii. I also know that drug traffickers and firearms traffickers commonly possess—on

their person, at their residences, at their places of business, in their vehicles, and other locations where they exercise dominion and control—firearms, ammunition, and records or receipts pertaining to such.

- iv. I know that firearms traffickers and drug traffickers often put their telephones in nominee names to distance themselves from telephones that are utilized to facilitate these and related offenses. I also know that firearm and drug traffickers often use proceeds to purchase assets such as vehicles, property, jewelry, and narcotics. I also know that firearm and drug traffickers often use nominees to purchase or title these assets to avoid scrutiny from law enforcement.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other investigators and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. There is probable cause to believe that evidence of violations of the following laws of the United States, including the items described in Attachment B, will be found in the property listed in Attachments A, respectively: 18 U.S.C. § 922(a)(1)(A) (engaging in the business of dealing and manufacturing of firearms without a license); 18 U.S.C. § 922(a)(5) (unlawful interstate transfer of a firearm); and 18 U.S.C. § 371 (conspiracy).

#### **Probable Cause**

- 7. On June 22, 2024, Milwaukee Police (MPD) Officers (Ofc.) responded to Aurora

Sinai Medical Center, 945 N. 12<sup>th</sup> Street, in Milwaukee, regarding a shooting victim. Upon arrival officers located and interviewed Marcus M. FRANKLIN (DOB XX/XX/2005).

8. FRANKLIN stated he currently resides at 630 N. Vel R. Phillips Avenue, Unit 812, Milwaukee, Wisconsin (PREMISES), with other members of his family, and he has resided there for four (4) years. FRANKLIN stated that on June 22, 2024, he drove himself to the hospital to seek treatment for an accidental self-inflicted gunshot wound to his left leg. FRANKLIN stated he accidentally shot himself on June 20, 2024, at his residence (PREMISES), while inside of his bedroom. FRANKLIN stated he was “finishing his project” of building a Polymer 9mm pistol. FRANKLIN further explained he “builds DIY guns” and described himself as a “gunsmith”. FRANKLIN explained that he learned how to build firearms by watching YouTube videos. FRANKLIN stated after he completed the build, he went to clean the firearm, and as he was disassembling the firearm he pulled the trigger, causing the accidental discharge. FRANKLIN stated he finished the firearm on June 21, 2024, and unassembled it to ship it. FRANKLIN explained that he had been sent a pre-paid shipping label to ship the completed firearm, via the United States Postal Service (USPS). FRANKLIN stated the package was shipped to a person named “John” who resided in Idaho, and he shipped it at the USPS location in downtown Milwaukee on Saint Paul Avenue.

9. Later in this same interview, FRANKLIN stated, “It’s a business, helping people build guns.” FRANKLIN also stated he goes to the shooting range with his mother, to test-fire the firearms that he builds for people. FRANKLIN continued to explain that his customers find him

through promotions on the social media apps such as Telegram, Instagram, and Facebook. FRANKLIN also stated he has a YouTube channel.

10. FRANKLIN stated he builds firearms utilizing various kits, explaining that “some people want smaller guns, some people want subcompact guns, and some people want compact guns.” FRANKLIN explained his customers buy the firearms parts-kits, and the manufacturers send the kits directly to FRANKLIN. FRANKLIN then completes the firearm and sends to the customer via a prepaid label, which is provided by the customer. FRANKLIN stated his customers send him part-kits from the companies Gorilla Machine, Polymer 80, Gunbuilders.com, and No Quarter. FRANKLIN stated he typically tells his customers that his turn-around time to build their firearms is two to three weeks. FRANKLIN stated his customers will send him multiple packages which contain a barrel and firing pin separate from the frame. FRANKLIN stated he uses a “dremel”, sander, and a cutter to complete the builds. FRANKLIN also stated he ships the firearms he builds from different post offices, and he also stated some of his customers are local to the Milwaukee area.

- i. Your affiant is aware that the companies Gorilla Machine, Polymer 80, Gunbuilders.com, and No Quarter all specialize in selling 80% firearms kits which are designed to be readily converted to a completed firearm.
- ii. Your affiant is further aware that when a firearm is capable of firing a round, it would have to be completed past the 80% legal threshold and would therefore be considered a fully functioning firearm.

11. During the interview with MPD, FRANKLIN stated he taught his girlfriend's brother how to build firearms and FRANKLIN stated that his girlfriend's brother is also now engaged in manufacturing firearms, in a similar manner to FRANKLIN.

12. FRANKLIN explained to MPD officers that his customers will typically spend approximately \$300 dollars for the firearm parts, to include the frame, slide, and upper and lower parts kits. FRANKLIN stated he charges the customer \$400 for a "full service" build, but stated he does sometimes give discounts. FRANKLIN further stated some customers only need half of a build, meaning half is already assembled and he only needs to complete the firearm. FRANKLIN stated people will often start to build a firearm, realize they cannot complete the build, and will need a "professional" to finish the build.

13. While at the hospital to interview FRANKLIN, officers located a vehicle that belonged to FRANKLIN. The vehicle is more particularly described as a 2020 Nissan Sentra four door sedan (VIN JN1AB8DV1LY205634, bearing Wisconsin license plate no. ATJ7945). The vehicle is registered to FRANKLIN.

#### **Consent Search of FRANKLIN's Residence**

14. On June 22, 2024, MPD Officers conducted a consent search at FRANKLIN's residence, 630 N. Vel R. Phillips, Unit 812, Milwaukee, Wisconsin. The consent to search form was signed by FRANKLIN and his mother N.S. (DOB XX/XX/1983). FRANKLIN declined to consent to a search of his vehicle (2020 Nissan Sentra four door sedan). During the search of the residence, officers located an intact bullet. Additionally, officers observed in the residence a rotary

“dremel” style tool, a “jig” for a compact lower Polymer 80 pistol, a Polymer 80 pistol compact lower receiver box, a Polymer 80 pistol lower receiver, ammunition, and an unknown metal firearm part. The USPS shipping label for the Polymer 80 pistol box indicated the kit was delivered to PREMISES on June 15, 2024, where USPS records state it was signed for by “M. FRANKLIN”. However, MPD did not recover or seize any of the aforementioned items.

- i. Your Affiant is aware through training and experience that the tools observed during this consent search would allow FRANKLIN to readily convert Polymer 80 parts kits into functioning firearms.

15. On June 28, 2024, at approximately 09:16 AM CST, Your Affiant observed the aforementioned Blue Nissan Sentra (bearing Wisconsin license plate no. ATJ7945), drive up and enter the parking garage for PREMISES. The garage door is activated by a garage door opener. Next to the parking garage entrance is a prominent sign which is labeled “Boston Lofts” which is the name of the apartment building of the PREMISES.

### **Conclusion**

16. Your Affiant is aware through training and experience that it is common for those who possess and traffic firearms, to utilize electronic media devices, which often possess cameras, to photograph and send messages to negotiate the purchase and sale of their firearms. Your Affiant is also aware that firearms are a commodity that are often held for long periods of time. As stated above, it is known that FRANKLIN utilized social media sites like Telegram, Instagram, and Facebook to engage in manufacture and trafficking of firearms and that he communicated with



customers utilizing electronic devices. It is common for those individuals engaged in trafficking of firearms to store electronic devices of all types at their home to facilitate their operation.

### **TECHNICAL TERMS**

17. Based on my training and experience, I use the following technical terms to convey the following meanings:

- i. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- ii. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- iii. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

18. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **PREMISES** in whatever form they are found. One

form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrants applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

19. *Probable cause.* I submit that if a computer or storage medium is found on the **PREMISES**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- i. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- ii. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- iii. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- iv. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

20. *Forensic evidence.* As further described in Attachment B, these applications seek permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrants, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **PREMISES** because:

- i. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- ii. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was

accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- iii. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- iv. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual

information necessary to understand other evidence also falls within the scope of the warrants.

- v. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

21. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrants. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- i. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrants call for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrants can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- ii. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- iii. Variety of forms of electronic media. Records sought under these warrants could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

22. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrants and would authorize a later review of the media or information consistent with the warrants. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrants.

23. Because several people share the **PREMISES** listed in Attachments A, it is possible that the **PREMISES** will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in these warrants could be found on any of those computers or storage media, the warrants applied for would permit the seizure and review of those items as well.

### **CONCLUSION**

24. I submit that this affidavit supports probable cause for warrants to search the following: the person of Marcus M. FRANKLIN (DOB XX/XX/2005); a 2020 Nissan Sentra four door sedan (VIN JN1AB8DV1LY205634, bearing Wisconsin license plate no. ATJ7945); and the premises located at 630 N. Vel R. Phillips, Unit 812, Milwaukee, Wisconsin, (“**PREMISES**”) as further described in Attachment A, and seize the items described in Attachment B.



**ATTACHMENT A**  
**Property to be searched**

1. The person of Marcus M. FRANKLIN
2. 2020 Nissan Sentra four door sedan (VIN JN1AB8DV1LY205634, bearing Wisconsin license plate no. ATJ7945)
3. The property to be searched is the premises located at 630 N. Vel R. Phillips, Unit 812, in Milwaukee, Wisconsin, any additional on-site storage units that are provided to the residents of the residence, sheds or on-site storage, and any vehicle located on the **PREMISES** under the control of Marcus M. FRANKLIN. Unit 812 is inside a multi-unit apartment building named Boston Lofts. Unit 812 is a two-floor loft style apartment with stairs leading to the second floor. See the below photograph depicting the outside of the apartment building:





**ATTACHMENT B**  
*Property to be seized*

All evidence pertaining to the violations of 18 U.S.C. § 922(a)(1)(A) (engaging in the business of dealing and manufacturing of firearms without a license); 18 U.S.C. § 922(a)(5) (unlawful interstate transfer of a firearm); and/or 18 U.S.C. § 371 (conspiracy), involving Marcus M.

FRANKLIN and his co-conspirators, including, but not limited to, the following:

1. Firearms;
2. Firearms parts kits;
3. Tools commonly used to manufacture and/or build firearms;
4. Documents or information related to the purchase, sale, and/or shipment of firearms, ammunition, or firearms accessories;
5. Photographs or other documents related to firearms, ammunition, or firearms accessories;
6. ATF Firearm Purchase Forms 4473, firearm boxes, bipods, tripods, upper receivers, receipts and any records related to firearms, firearms accessories, ammunition, financial documents that transfer of proceeds of the above schemes, computers, electronics capable of communication, and cellphones such as:
  - a. lists of contacts and any identifying information;
  - b. photographs, videos, or other media storage connected to firearms;
  - c. types, amounts, and prices of firearms purchased/sold;
  - d. any information related to sources or purchasers of firearms (including names, addresses, phone numbers, or any other identifying information);

- e. all bank records, checks, credit card bills, account information, and other financial records related to firearms commerce;
  - f. any and all financial records connected to the purchase/sale of firearms;
7. Cellphones, computers, and all media storage devices that may hold documentation regarding firearm or ammunition purchases/sales and customers;
8. Any and all financial records connected to the purchase/sale of firearms, and any correspondence between suspects and other firearms sellers and/or purchasers;
9. All bank records, checks, credit card bills, account information, and other financial records related to firearms commerce;
10. Proceeds of firearms trafficking activities, including United States currency;
11. All bank records, checks, credit card bills, account information, and other financial records; Financial records, documents, statements, or other evidence of control of bank or other financial accounts and investment funds;
12. Personal address books, telephone bills, photographs, letters, personal notes, documents and other items or lists reflecting names, addresses, telephone numbers, addresses and communications regarding illegal activities among and between members and associates involved in firearms trafficking activities;
13. Documents and deeds reflecting the purchase or lease of items obtained with the proceeds from firearm trafficking activities;
14. Records of off-site locations to store proceeds and other records, including safes, vaults, or lock boxes, safe deposit box keys, records and receipts and rental agreements for storage facilities;

15. Records of mail and communications services, cellular telephones and all electronic storage areas on the device including stored telephone numbers, recently called numbers list, text messages, digital audio and or video recordings, pictures, settings, and any other user defined settings and/or data;

16. Indicia of occupancy, residency or ownership of the premises, including utility bills, telephone bills, loan payment receipts, addressed envelopes, escrow documents and keys;

17. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

18. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

19. All records relating to violations of 18 U.S.C. § 922(a)(1)(A) (engaging in the business of dealing and manufacturing of firearms without a license); 18 U.S.C. § 922(a)(5) (unlawful interstate transfer of a firearm); and/s 18 U.S.C. § 371 (conspiracy), involving Marcus M. FRANKLIN:

- a. Records and information relating to a conspiracy to violate the laws of the United States, including the scope, manner, means, acts in furtherance, and identity of any co-conspirators;
- b. Records and information relating to the identity or location of FRANKLIN’s co-conspirators;

- c. Records and information relating to communications with Internet Protocol addresses;
  - d. Records and information relating to the crimes referenced in Attachment B, paragraph 19; and
  - e. Records and information relating to intent or state of mind.
20. Computers or storage media used as a means to commit the violations described above;
21. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;

- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

22. As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

23. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

24. The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.



## Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

## Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

---

*Executing officer's signature*

---

Printed name and title



**ATTACHMENT A**  
**Property to be searched**

1. The person of Marcus M. FRANKLIN
2. 2020 Nissan Sentra four door sedan (VIN JN1AB8DV1LY205634, bearing Wisconsin license plate no. ATJ7945)
3. The property to be searched is the premises located at 630 N. Vel R. Phillips, Unit 812, in Milwaukee, Wisconsin, any additional on-site storage units that are provided to the residents of the residence, sheds or on-site storage, and any vehicle located on the **PREMISES** under the control of Marcus M. FRANKLIN. Unit 812 is inside a multi-unit apartment building named Boston Lofts. Unit 812 is a two-floor loft style apartment with stairs leading to the second floor. See the below photograph depicting the outside of the apartment building:



**ATTACHMENT B**  
*Property to be seized*

All evidence pertaining to the violations of 18 U.S.C. § 922(a)(1)(A) (engaging in the business of dealing and manufacturing of firearms without a license); 18 U.S.C. § 922(a)(5) (unlawful interstate transfer of a firearm); and/or 18 U.S.C. § 371 (conspiracy), involving Marcus M.

FRANKLIN and his co-conspirators, including, but not limited to, the following:

1. Firearms;
2. Firearms parts kits;
3. Tools commonly used to manufacture and/or build firearms;
4. Documents or information related to the purchase, sale, and/or shipment of firearms, ammunition, or firearms accessories;
5. Photographs or other documents related to firearms, ammunition, or firearms accessories;
6. ATF Firearm Purchase Forms 4473, firearm boxes, bipods, tripods, upper receivers, receipts and any records related to firearms, firearms accessories, ammunition, financial documents that transfer of proceeds of the above schemes, computers, electronics capable of communication, and cellphones such as:
  - a. lists of contacts and any identifying information;
  - b. photographs, videos, or other media storage connected to firearms;
  - c. types, amounts, and prices of firearms purchased/sold;
  - d. any information related to sources or purchasers of firearms (including names, addresses, phone numbers, or any other identifying information);

- e. all bank records, checks, credit card bills, account information, and other financial records related to firearms commerce;
  - f. any and all financial records connected to the purchase/sale of firearms;
- 7. Cellphones, computers, and all media storage devices that may hold documentation regarding firearm or ammunition purchases/sales and customers;
  - 8. Any and all financial records connected to the purchase/sale of firearms, and any correspondence between suspects and other firearms sellers and/or purchasers;
  - 9. All bank records, checks, credit card bills, account information, and other financial records related to firearms commerce;
  - 10. Proceeds of firearms trafficking activities, including United States currency;
  - 11. All bank records, checks, credit card bills, account information, and other financial records; Financial records, documents, statements, or other evidence of control of bank or other financial accounts and investment funds;
  - 12. Personal address books, telephone bills, photographs, letters, personal notes, documents and other items or lists reflecting names, addresses, telephone numbers, addresses and communications regarding illegal activities among and between members and associates involved in firearms trafficking activities;
  - 13. Documents and deeds reflecting the purchase or lease of items obtained with the proceeds from firearm trafficking activities;
  - 14. Records of off-site locations to store proceeds and other records, including safes, vaults, or lock boxes, safe deposit box keys, records and receipts and rental agreements for storage facilities;

15. Records of mail and communications services, cellular telephones and all electronic storage areas on the device including stored telephone numbers, recently called numbers list, text messages, digital audio and or video recordings, pictures, settings, and any other user defined settings and/or data;

16. Indicia of occupancy, residency or ownership of the premises, including utility bills, telephone bills, loan payment receipts, addressed envelopes, escrow documents and keys;

17. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

18. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

19. All records relating to violations of 18 U.S.C. § 922(a)(1)(A) (engaging in the business of dealing and manufacturing of firearms without a license); 18 U.S.C. § 922(a)(5) (unlawful interstate transfer of a firearm); and/s 18 U.S.C. § 371 (conspiracy), involving Marcus M. FRANKLIN:

- a. Records and information relating to a conspiracy to violate the laws of the United States, including the scope, manner, means, acts in furtherance, and identity of any co-conspirators;
- b. Records and information relating to the identity or location of FRANKLIN’s co-conspirators;

- c. Records and information relating to communications with Internet Protocol addresses;
  - d. Records and information relating to the crimes referenced in Attachment B, paragraph 19; and
  - e. Records and information relating to intent or state of mind.
20. Computers or storage media used as a means to commit the violations described above;
21. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;

- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

22. As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

23. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

24. The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.